UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JANE DOE,

Plaintiff,

v.

EATING RECOVERY CENTER LLC,

Defendant.

Case No. 23-cv-05561-VC

ORDER GRANTING EATING RECOVERY CENTER'S MOTION FOR SUMMARY JUDGMENT ON DOE'S CIPA CLAIM

Re: Dkt. Nos. 86, 100, 108, 119, 149, 152

The California Invasion of Privacy Act (CIPA) was enacted in 1967 to criminalize wiretapping and eavesdropping on confidential communications. Although it is a criminal statute, CIPA also authorizes victims to bring civil actions against those who violate the statute, allowing recovery of civil penalties of $5,000 per violation or three times the amount of actual damages—whichever is greater. *See* Cal. Penal Code § 637.2(a).

The language of CIPA is a total mess. It was a mess from the get-go, but the mess gets bigger and bigger as the world continues to change and as courts are called upon to apply CIPA's already-obtuse language to new technologies. Indeed, we have reached the point where it's often borderline impossible to determine whether a defendant's online conduct fits within the language of the statute.

This is such a case. The plaintiff seeks to impose CIPA liability on a website operator for using a third party to perform data analytics and targeted advertising. In particular, liability here turns on whether the third party "read" or "attempt[ed] to read" or attempted "to learn" the contents of an internet communication between the plaintiff and the website operator while that communication was "in transit." If so, the website operator could be liable to the plaintiff under

CIPA for enabling the third party to engage in that conduct.

As discussed in this ruling, the statutory language at issue here is ambiguous. One could imagine an interpretation under which the website operator would be liable. But CIPA is a criminal statute. When courts are called upon to interpret ambiguous criminal statutes in California, the rule of lenity applies—even when the statute is being invoked in a civil action. *Harrott v. County of Kings*, 25 Cal. 4th 1138, 1154 (2001). Courts are also supposed to narrowly construe civil statutes that impose punitive civil penalties. *See Hale v. Morgan*, 22 Cal. 3d 388, 401 (1978). So the Court will adopt a narrower but equally reasonable interpretation of CIPA—one that does not encompass the conduct at issue in this case.

The state of affairs with CIPA is untenable. Courts are issuing conflicting rulings, and companies have no way of telling whether their online business activities will subject them to liability. That seems particularly true of Penal Code Section 631(a), the CIPA provision at issue here. The California Legislature needs to step up. It would be bad enough if CIPA were merely a civil statute that allowed plaintiffs to recover actual damages for violations. But CIPA imposes criminal liability and punitive civil penalties. Under these circumstances, it is imperative for the Legislature to bring CIPA into the modern age and to speak clearly about how the kinds of activities at issue in this case should be treated. Until that happens, courts should generally resolve CIPA's many ambiguities in favor of the narrower interpretation.

I

A

The Meta Pixel is a piece of code that can be installed on a website to track how visitors interact with that website. When visitors take certain actions on a website, the Pixel transmits information related to those actions to Meta, which in turn uses the information to provide various services for the website operator. A common reason website operators use the Pixel is to target ads to people likely to purchase their products or services.

At a high level, the process for collecting and using Pixel data involves three steps. First, certain information about a visitor's activity on the website, which Meta refers to as "event

data," is captured and shared with Meta. Website operators choose what data to send to Meta, and Meta filters that data to lower the risk of storing personally identifiable information. Next, Meta attempts to match event data with Meta user accounts. Event data about a particular visitor can be matched with that visitor's Meta account only if the visitor is logged into their Meta account at the time they are visiting the website. Finally, event data can be used by Meta in various ways, depending on the website operator's preferences. Event data can potentially be used: (1) to identify Meta users to send ads to; (2) to provide aggregated data to website operators about actions users take on their websites; and (3) as an input into Meta's machine learning algorithms for optimizing Meta's content delivery.

With respect to ad targeting, Meta uses event data matched with Meta accounts to create "audiences" to send (or not send) ads to, based on criteria selected by the website operator. For instance, a website operator can define a group it wants to show ads to (an "inclusive custom audience") or a group it specifically does not want to send ads to (an "exclusive custom audience"). Meta can also send ads to Meta users with relevant traits similar to those in a previously created custom audience (a "lookalike audience").

B

Eating Recovery Center (ERC) is a company that treats people for eating disorders. It used the Pixel on its website from 2019 to 2024. ERC's stated goal in using the Pixel was to increase the efficacy of its internet advertising and to try to help people in need of ERC's services. ERC installed the standard version of the Pixel, that is, without configuring it to transmit event data other than what the Pixel captures by default. This default event data includes, for each visitor to ERC's website: (1) the specific URL of each page browsed by the visitor; (2) the amount of time the visitor spent on the page; (3) the path the visitor took to get to that page, *i.e.*, the URL of the page they came from; and (4) certain actions, such as button clicks or inputted answers, on some pages.[1]

[1] A URL, or a "Universal Resource Locator" is the web address of a document or webpage on the internet. For example, the following URL belongs to a page about ERC's eating disorder

The event data collected by ERC was used to create custom audiences for targeting ERC ads to Meta users. For example, ERC often used an inclusive custom audience to send ads to people who had visited its website within the last 180 days. At the same time, during the period at issue, ERC stated on its website that communications with ERC were "100% confidential," that it would not collect visitors' personal information while they visited the website, and that it would "NEVER share or sell [visitors'] personal information to a third party of any nature."

C

Jane Doe is a California resident who was diagnosed with anorexia in 2021. In June 2022, she visited ERC's website, apparently to consider treatment options. On the same day she first visited ERC's website, Doe began receiving ads on Facebook from ERC and other mental health services.[2] Doe filed this proposed class action lawsuit in October 2023, asserting statutory claims based on CIPA, the California Medical Information Act (CMIA), and the California Unfair Competition Law (UCL). She also asserted a common law unjust enrichment claim. At the pleading stage, the UCL claim was dismissed because Doe did not plausibly allege that she suffered any economic injury from ERC's conduct. The CIPA, CMIA, and unjust enrichment claims survived.

Now the parties have filed cross-motions for summary judgment. Doe argues that the Court should grant summary judgment for her on her CIPA and CMIA claims. ERC, for its part, says it's entitled to summary judgment on all remaining claims.[3] This ruling addresses only the

---

treatment centers in California: https://www.eatingrecoverycenter.com/recovery-centers/california. URLs typically include the website name ("www.eatingrecoverycenter.com" in the example), the path to the specific page or document ("/recovery-centers/california" in the example), and can also include optional elements like query strings, which convey additional information to the web server, often to customize web pages or to track user activity.

[2] Doe received one ad from ERC on June 14, 2022. She received three ERC ads in February–March 2023 and another eleven ERC ads in June–August 2023.

[3] ERC also argues that Doe does not have standing to bring this case, but that's wrong. Whether there is Article III standing in privacy cases based on browsing activity depends on whether the activity is private or personal enough. *See Lineberry v. AddShopper, Inc.*, 2025 WL 551864, at *1 (N.D. Cal. Feb. 19, 2025). The URLs at issue in this case convey information that is personal enough to confer Article III standing. There may not be standing to sue based on a disclosure that a plaintiff was shopping for a football jersey, but there's standing to sue based on a disclosure that a plaintiff was likely shopping for eating disorder services.

CIPA claim; ERC's motion for summary judgment on the other claims will be granted in a separate ruling.

II

CIPA was enacted in 1967 to address the increasing use of wiretapping to eavesdrop on private phone conversations. Although CIPA is located in the California Penal Code and creates criminal liability, it also allows a private party injured by conduct proscribed by the statute to bring a civil suit to recover damages and civil penalties. Cal. Penal Code § 637.2. In recent years, the statute has frequently been invoked—with mixed success—to challenge the use of third-party software that records website activity without visitors' knowledge. *Compare Heerde v. Learfield Communications*, 741 F. Supp. 3d 849 (C.D. Cal. 2024), *with Gutierrez v. Converse Inc.*, 2024 WL 3511648 (C.D. Cal. July 12, 2024), *aff'd*, 2025 WL 1895315 (9th Cir. July 9, 2025).

Two CIPA provisions, Penal Code Sections 631 and 632, can potentially be construed to create liability for website operators who use tracking software on their websites. Section 631—specifically, Section 631(a)—is the provision asserted by Doe in this case.[4] Section 631(a) contains four clauses, each of which can give rise to liability. It imposes liability on anyone who:

> (1) ". . . intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument";
>
> (2) "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state";
>
> (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained"; or
>
> (4) "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

[4] Section 632 is not directly at issue in this case, but it is implicated by ERC's arguments about how to read Section 631. Section 632 creates liability for anyone who eavesdrops upon or records a confidential communication without the consent of all parties to the communication. Although Section 631 is more typically litigated in CIPA cases against website operators, Section 632 has also been invoked in this context. *See, e.g.*, *Smith v. YETI Coolers, LLC*, 754 F. Supp. 3d 933, 943–44 (N.D. Cal. 2024); *Smith v. Rack Room Shoes, Inc.*, 2025 WL 1085169, at *5 (N.D. Cal. Apr. 4, 2025); *Shah v. Capital One Finance Corporation*, 768 F. Supp. 3d 1033, 1054 (N.D. Cal. 2025).

Cal. Penal Code § 631(a).

The first clause is not implicated here because nobody tapped a "telegraph or telephone wire, line, cable, or instrument." *See Swarts v. Home Depot, Inc.*, 689 F. Supp. 3d 732, 743 (N.D. Cal. 2023) (collecting cases). But Doe argues that Meta violated the second clause because Meta read, attempted to read, or attempted to learn the contents of her communications with ERC while they were in transit (and without her consent). Thus, Doe contends, ERC is liable under the fourth clause for aiding Meta and/or conspiring with Meta to violate the second clause. Doe also contends that Meta violated the third clause, which involves using information acquired in violation of the second clause, and that ERC is also liable for that under the fourth clause. But there can be no violation of the third clause without a violation of the second clause. So, the threshold question is whether Meta violated the second clause of Section 631(a).

The parties dispute two elements of the second clause. First, should the event data obtained by Meta be considered the "contents" of Doe's communication with ERC? Second, did Meta read, attempt to read, or attempt to learn this information while it was "in transit"? If the answer is indisputably "yes" to both these questions, Doe is entitled to summary judgment. If the answer is indisputably "no" for either of those questions, ERC is entitled to summary judgment.

As discussed below, the event data that Meta obtained when Doe visited ERC's website is, as a matter of law, the contents of a communication. The harder question is whether the communications were in transit when Meta read, attempted to read, or attempted to learn their contents. This question is hard because the statute was not drafted with the internet in mind. It is also hard because, even aside from the internet issue, the statute is just badly drafted. The Court concludes, albeit without a great deal of confidence, that Meta's conduct did not satisfy the "in transit" requirement as a matter of law.

A

According to the Ninth Circuit, the term "contents" of a communication under CIPA has the same meaning as the parallel term in the federal Wiretap Act. *See In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 607 (9th Cir. 2020). The Wiretap Act defines the

contents of a communication as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

As described above, Meta obtained the following information related to Doe's interactions with ERC's website: (1) the specific URL of each page Doe browsed; (2) the time Doe spent on each page; (3) the path Doe took to get to that page; and (4) certain actions, such as button clicks. The captured URLs and the information related to those URLs are sufficient to qualify as contents of a communication under the second clause of Section 631(a).[5]

The Ninth Circuit has distinguished URLs that include "search term[s] or similar communication[s]," which can constitute the contents of a communication, from those that include only basic identification and address information. *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1108–09 (9th Cir. 2019). Several courts have held that detailed URLs that reveal the specific document, product, or service that a user is viewing count as contents of communications. *See, e.g.*, *Yoon v. Meta Platforms, Inc.*, 2024 WL 5264041, at *5 (N.D. Cal. Dec. 30, 2024); *In re Meta Pixel Healthcare Litigation*, 647 F. Supp. 3d 778, 795–96 (N.D. Cal. 2022); *Lineberry*, 2025 WL 551864, at *3. As in those cases, the URLs here reveal enough information to be deemed contents of communications. They reveal that Doe researched anorexia, explored treatment options and locations, and at least clicked through to a self-assessment form.[6] Especially considering that the data associated with the URLs also shows Doe's browsing path and how long she spent on each page, the URL-related data obtained by

[5] Apart from the URL-related data, Meta also obtained information related to some actions Doe took on the website, such as clicking on the "For Me" button under the prompt "I am reaching out . . . " on a page with a self-assessment form. The parties dispute the significance of this information. ERC points out that Meta received only the answer Doe chose, but not the prompt. ERC argues that because there is no evidence showing that Meta could or tried to determine the question underlying Doe's "disembodied" answer, it cannot be enough to constitute the contents of a communication. Doe asserts that the answer alone is the content of the communication, and that Meta would have been capable of making the simple connection between Doe's answer and the question reflected on the page. Doe's position seems right, but in any event, the URL-related data is enough to satisfy the "contents of communication" requirement.

[6] The parties dispute whether Doe actually filled out the self-assessment form. Although Doe testified that she thought she filled out the form, the data produced by Meta does not show that Doe filled out the form.

Meta conveys far more than basic identification and address information. It conveys a significant possibility that Doe had anorexia at the time she visited the ERC website.

B

The next question is whether Meta read, attempted to read, or attempted to learn the contents of the communications between Doe and ERC while the communications were in transit. It's unclear how to apply the transit requirement to instantaneous internet communications. Courts (including probably this one) have been all over the map on the issue. Some seem to say that merely intercepting the communication while it's being made is enough, as long as the interception happens simultaneously or near-simultaneously. *See, e.g.*, *Heerde*, 741 F. Supp. 3d at 862; *Esparza v. UAG Escondido A1 Inc.*, 2024 WL 559241, at *3 (S.D. Cal. Feb. 12, 2024). Others say that you also have to "read" the communication while it's in transit—that is, you have to do something more than just intercept the contents of the communication or redirect them to yourself during the virtually infinitesimal amount of time it takes for the communication to travel from the website visitor to the website operator. *See Torres v. Prudential Financial*, 2025 WL 1135088, at *5–7 (N.D. Cal. Apr. 17, 2025); *see also Gutierrez*, 2024 WL 3511648, at *7. For example, in *Torres*, Judge Breyer ruled that the in-transit requirement was not satisfied when a third-party company intercepted communications and stored them in a server because the company didn't actually read or attempt to read the communications while they were in transit. *See* 2025 WL 1135088, at *5.

Doe's first argument is that, even if Judge Breyer's interpretation of Section 631(a) is correct, Meta read her communications while they were in transit. Meta's corporate representative testified that, before logging the data that it obtains from websites, Meta filters URLs to remove information that it does not wish to store (including information that Meta views as privacy protected). Doe asserts that this step, which occurs after Meta obtains the data but before the data is stored, amounts to reading the communication while in transit.

There are a couple of reasons why that is wrong as a matter of law. First, Meta's automated effort to avoid storing material that it should not be storing can't reasonably be

considered "reading" or "learning" the contents of the communication. Reading or learning the contents of a communication requires "some effort at understanding the substantive meaning" of the communication. *Williams v. DDR Media*, LLC, 757 F. Supp. 3d 989, 995 (N.D. Cal. 2024). A filtering process that simply sorts out certain data—which may be better analogized to sorting mail than to reading it—can't fairly be characterized as an effort at understanding the meaning of the communication. Second, the filtering operation indisputably takes place after the communication has already traveled from the website visitor to the website operator. The parties agree that event data is transmitted to Meta about 0.2 seconds after the visitor's action is transmitted to the website. The filtering of the data necessarily happens after this because the event data is encrypted while being sent to Meta. Encrypted data is sent in packets that have to be reassembled before anything can be done with the data. Thus, Meta has to receive the packets of data and reassemble them before it can filter and log the data. Doe doesn't dispute that this is how the technology works; rather, she disputes how it should be characterized. Doe argues that the communication remains in transit until after it goes through Meta's filtering process and is logged by Meta. But the only commonsense meaning of transit, at least in the context of this statute, is the transit from the person sending the communication to its intended recipient.

It's worth pausing here to acknowledge how strange this outcome is. Regardless of whether it is receiving the communication a second before or after it reaches the website, Meta is effectively engaging in the same conduct. Arguably, then, the purpose of the statute can only be effectuated by reaching the same result in both instances. This argument would have a place if the language were ambiguous. But "in transit" is not ambiguous. And that's the problem with cases involving the tracking of online activity—the statutory language was drafted with very different technology in mind, and it does not map properly onto the internet.[7]

Doe makes a secondary argument that is potentially stronger—an argument that seemingly goes beyond what Judge Breyer considered in *Torres*. At the hearing on this motion,

[7] Even if the "in transit" concept were ambiguous, the Court would adopt the narrow construction for the reasons discussed in this ruling.

the Court asked the parties to address the language from the second clause of Section 631(a) that is not discussed in *Torres*—namely, the language that imposes liability for attempting "to learn" the contents of the communication while the communication is in transit. In response, Doe now argues that the statute does not require the communication to be actually read or learned while it is in transit; it is enough to intercept the communication with the intent to learn its contents later.[8] To use the pertinent language of the second clause of Section 631(a), liability is imposed whenever someone "willfully and without the consent of all parties . . . attempts . . . to learn the contents or meaning of any . . . communication while the same is in transit." Applying this language, the argument goes, if someone intercepts a communication as part of an attempt to learn its contents, it doesn't matter whether the learning occurs while the communication is still in transit or later on, because the interception is still part of an "attempt to learn" the contents of the communication.

With the caveat that it's virtually impossible to understand what Section 631(a) actually means, that appears to be a plausible interpretation, particularly when considering the language in isolation. But in context, the better conclusion is that you must do something more than just intercept the communication while it is in transit to be held liable. That is in part because of the CIPA provision that immediately follows Section 631. As mentioned earlier, Section 632 makes it unlawful to "eavesdrop upon or record" a "confidential communication" without the consent of all parties to the communication. Intercepting the contents of a communication and recording those contents (as Doe alleges Meta does) would seem to be covered by Section 632. If the same conduct were covered by the second clause of Section 631(a), it would appear to render Section 632 superfluous—at least as applied to the type of internet communication at issue here. This is one reason why ERC's reading of the second clause of Section 631(a)—and Judge Breyer's application of it in *Torres*—makes more sense.

[8] To be clear, the Court contemplated this interpretation during the hearing on this motion and invited the parties to submit supplemental briefing on this specific aspect of the statutory language.

There is an even more important reason to avoid reading the second clause of Section 631(a)—and, for that matter, any portion of CIPA—too broadly: it is a criminal statute. Even though most CIPA cases are private civil actions, the interpretations courts adopt while adjudicating those actions could affect the extent to which people or companies are subject to criminal liability. "When the governing standard is set forth in a criminal statute, it is appropriate to apply the rule of lenity in resolving any ambiguity in the ambit of the statute's coverage." *Harrott*, 25 Cal. 4th at 1154; *see also Bittner v. United States*, 598 U.S. 85, 103 (2023) (Gorsuch J., joined by Jackson, J.) (In the context of a statute that imposes both criminal and civil penalties based on the same statutory term, "the rule of lenity, not to mention a dose of common sense, favors a strict construction.").[9] A similar principle applies to civil statutes that impose punitive civil penalties. *See Hale*, 22 Cal. 3d at 401 ("Uniformly, we have looked with disfavor on ever-mounting penalties and have narrowly construed the statutes which either require or permit them."); *see also People v. Mobil Oil Corporation*, 143 Cal. App. 3d 261, 276 (1983) (narrowly construing a statute imposing a "substantial civil penalty" of $500 per violation).

Indeed, there is reason to question whether the Legislature intended for CIPA to apply to the type of conduct implicated by this case at all. Recall that CIPA was enacted in 1967. Its language—with words like "read" and "intercept" and "in transit"—is ill-suited for application to internet communications. The Legislature has never, in over four decades, amended Section 631 to adapt its language to the digital age.[10] And California has since adopted other statutes that more clearly speak to the practice of data sharing. *See* Cal. Civil Code § 1798.100 *et seq.*

[9] ERC does not argue that CIPA is unconstitutionally vague. But this potential constitutional concern may well provide another related reason to adopt the narrower of two alternative interpretations of CIPA's ambiguous language.

[10] Section 631 was amended in 1988 to authorize interception of wire communications by law enforcement officers in certain circumstances. *See* 1988 Cal. Legis. Serv. 111 (S.B. 1499); 1988 Cal. Legis. Serv. 1373 (S.B. 83). It was amended again in 1992 to provide that a defendant previously convicted of a violation of certain provisions of CIPA would be subject to the increased punishment specified in Section 631. *See* 1992 Cal. Legis. Serv. 298 (A.B. 2465). In 2011, it was amended to modify the terms of imprisonment under the statute. 2011 Cal. Legis. Serv. 15 (A.B. 109). Finally, it was amended in 2022 to exempt telephone companies from liability. 2022 Cal. Legis. Serv. 27 (S.B. 1272).

(California Consumer Privacy Act). To be sure, as Doe notes, CIPA was intended to protect Californians' privacy rights in the face of "the development of new devices and techniques for the purpose of eavesdropping upon private communications." Cal. Penal Code § 630. But using a third-party company to perform data analytics for web traffic is worlds different from wiretapping and eavesdropping. Did the Legislature really intend to subject companies like ERC to criminal liability for using third-party software to track website activity? Did it really mean to criminalize the use of web traffic data? Given the statute's ambiguity and its imposition of criminal liability, perhaps courts should not be so quick to assume that the answer is yes. But regardless of whether CIPA could, in some circumstances, impose criminal liability on website operators and data analytics firms for the transmission of information about web traffic and the subsequent use of that information, it would not be appropriate to interpret the "in-transit" requirement of Section 631(a) so broadly as to cover the conduct at issue here.

III

As difficult as it is to apply CIPA to the physical world, it's virtually impossible to apply it to the online world. Hopefully, the Legislature will go back to the drawing board on CIPA. Indeed, it would probably be best to erase the board entirely and start writing something new. But until that happens, courts should not contort themselves to fit the type of conduct alleged in this case into the language of a 1967 criminal statute about wiretapping. Because the evidence is undisputed that Meta did not read, attempt to read, or attempt to learn the contents of Doe's communications with ERC while those communications were in transit, ERC is entitled to summary judgment on Doe's CIPA claim. Doe's motion for summary judgment as to her CIPA claim is accordingly denied.

IT IS SO ORDERED.

Dated: October 17, 2025

VINCE CHHABRIA
United States District Judge